DATA SHEET

Tigera CNX

Secure Application Connectivity for the Cloud Native World

At A Glance

Tigera CNX™ provides secure application connectivity across multi-cloud and legacy environments, with the enterprise control and compliance capabilities required for mission critical deployments.

- Enables compliance with corporate security and regulatory requirements
- Consistent security policies applied across all compute environments
- Dynamically minimizes attack surface with real-time updates applied in milliseconds as policies are updated and workloads are created/ destroyed
- Protects against untrusted workloads and networks
- Enables multi-cloud connectivity and security, with legacy platform interoperability
- Operational simplicity enables automated, at-scale production
- Cloud native architecture with a horizontally-scalable, fully distributed control plane

Overview

In an increasingly cloud native world, applications are becoming more distributed, dynamically orchestrated, and run across multi-cloud infrastructure. To protect workloads and ensure compliance, connectivity must be established and secured in a highly dynamic environment that includes microservices, containers and virtual machines.

Tigera CNX™ provides secure application connectivity across multi-cloud and legacy environments, with the enterprise control and compliance capabilities required for mission critical deployments.

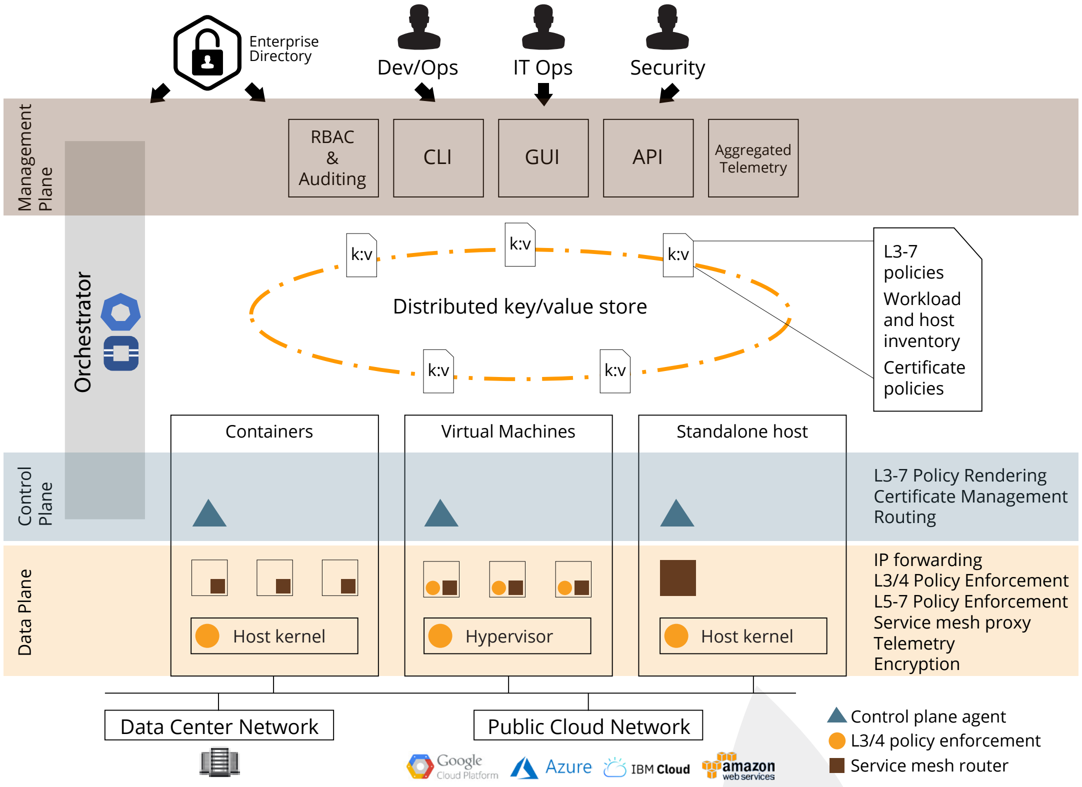
At the heart of CNX is Tigera's ZT-Auth™ technology, which enforces both filtering and encryption at multiple levels throughout the application connectivity stack: within the application, and on every container, virtual machine, and host network interface. The result is a ground-up Zero Trust security model built for the cloud native world, that also spans legacy virtualization and standalone host environments.

Tigera CNX was designed from the ground up as a cloud native solution, building on leading open source projects including Kubernetes, Calico and Istio. It connects and secures container, virtual machine and bare metal host workloads in public cloud and private data centers.

Highlights

- **Cloud Native Architecture.** CNX is the first secure application connectivity solution designed from the ground-up for cloud native environments, including multi-cloud deployments, while also protecting legacy applications running on virtual machines and bare metal hosts.
- **Zero Trust Security.** CNX's unique ZT-Auth™ technology enables organizations to move towards a Zero Trust approach to application connectivity, with multiple levels of policy enforcement and encryption enabling maximum security — independent of the underlying network infrastructure.
- **Enterprise Control and Compliance.** CNX provides the hierarchical, access-controlled policy controls required to integrate with existing organizational processes and meet internal and external compliance requirements.
- **Operational Simplicity.** CNX turns the complex, opaque SDN model of network virtualization and security on its head. CNX leverages proven kernel routing features for optimal reliability and visibility, with the operational tools required for rapid problem diagnosis and resolution.

Architecture and Key Components



CNX Architecture

The CNX architecture comprises the following high level elements:

- The **management layer** (CNX Manager) implements a unified, access-controlled management experience across command line, REST API and graphical user interfaces.
- The **key-value store** provides storage and distribution of global state (including policies and workload/host inventory) and the decoupling of the management layer from the control plane. CNX can be configured to use a dedicated or shared etcd store directly or via the Kubernetes API using custom resources[1].
- The **control plane** comprises a set of agents (CNX Nodes) deployed on each host in the cluster. The CNX Node controls functions local to its host, including real-time rendering of security policies, integration with host-local orchestrator functions and peering to network underlay. All this is accomplished in a fully distributed fashion, without any centralized SDN controller, resulting in CNX's exceptional scalability, fault tolerance and reliability.
- The **data plane** enforces security at the edge of every application, container, virtual machine and host-based service. It employs a flat IP networking model using native operating system data forwarding and filtering capabilities, with optional overlay and public cloud network integration for compatibility with all cloud and legacy environments.

[1] Note: Kubernetes API option only supported for deployments where all workloads are in a single Kubernetes cluster, and where Kubernetes IP address management is used (CNX IPAM features not supported)

Features and Benefits

Features	Benefits
Zero Trust Security	
• Flexible, label-based application policy model • Policy enforcement at multiple locations - edge of application, container, virtual machine and host interfaces • Certificate-based authentication, authorization and encryption*	• Enables compliance with corporate security requirements • Dynamically minimizes attack surface • Protects against untrusted underlying network
Multi-cloud & Legacy Platform Support	
• Multi-cloud support (public and private) • Multi-orchestrator (Kubernetes, OpenStack*, ...) • Deploy in container, virtual machine, and non-virtualized environments	• Enables adoption of multi-cloud strategy without compromising security • Ensures consistent policy enforcement across all environments • Facilitates seamless coexistence of cloud native and legacy applications
Enterprise Controls and Compliance	
• Hierarchical, multi-tier, Role-based Access Control (RBAC) security policies • Policy Violation Alerting with time series reporting, configurable thresholds and alert destinations • Policy Audit Mode — options include logging with or without enforcement • Configuration Auditing* — audit trail of all policy/configuration changes	• Minimizes organizational disruption of moving to cloud native architecture • Reduces time-to-deployment by parallelizing security policy decisions by developers, operations & security teams • Ensures compliance with internal governance & compliance requirements • Detects anomalous behavior earlier — before critical resources are accessed • Ensures security policies work as expected prior to enforcement
Operational Simplicity	
• Flat IP networking model (non-overlay, with optional IP-IP or VxLAN overlay) • Linux kernel data plane for forwarding and filtering • Flexible IP address management with support for IPv4 and IPv6 • Underlay network peering via border gateway protocol (BGP) • Policy Query Utility (calicoq) • REST API for programmatic control • Sidecar deployment model for service proxy*	• Provides full visibility into traffic routing • Minimizes learning curve for existing system administrators • Delivers optimal application performance • Enables rapid time to resolution • Reliably deploy at scale with automation of network and application security • Avoids changes to application to enable firewalling and encryption

Packages

CNX is available in two editions: Advanced and Enterprise.

	CNX Advanced	CNX Enterprise
Term	**Per node, annual subscription**	
Zero Trust Network Security		
Certificate-based authentication & authorization*	•	•
Flexible, label-based application policy model	•	•
Hierarchical network (L3-4) policy model	•	•
Hierarchical unified application (L3-7) policy model*		•
Multi-layer encryption (mTLS and host-based IPsec)*		•
Multi-Cloud and Lagacy Platforms		
Multi-Orchestrator support	•	•
Container, VM and non-virtualized workload support	•	•
Multi-cloud support	•	•
Federation*	•	•
Enterprise Control and Compliance		
Hierarchical, multi-tier, RBAC-controlled security policies	•	•
Policy alerting and verification	•	•
Auditing	•	•
Operational Simplicity		
Non-overlay, flat IP networking	•	•
Linux kernel data plane for forwarding and filtering	•	•
CNX manager GUI, REST API & diagnostics for L3–4 policies	•	•
CNX manager GUI, REST API & diagnostics for L3–7 policies*		•
Support		
Standard SLA - business hours	•	•
Premium SLA - 24-7 business-critical	•	•

Supported Platforms

Orchestrators

- Kubernetes 1.8, 1.9*
- OpenShift 3.7, 3.8*
- OpenStack* Ocata, Pike
- Any virtual machine orchestrator (including VMware vSphere) within VMs running one of the Operating Systems supported by CNX
- DC/OS*

Operating Systems

- RHEL 7.x
- CentOs 7.x
- Ubuntu 16.04
- Debian 8.x
- CoreOS Container Linux (latest stable)
- Windows Server 2016*

Cloud Infrastructure

Tigera CNX is compatible with all major public cloud infrastructure including:

- AWS EC2
- Microsoft Azure
- Google Cloud Platform
- IBM Cloud

Contact

For more information about Tigera CNX and how it can help you to achieve secure application connectivity in your environment, email us at contact@tigera.io or call us at +1 (415) 612-9546.

About Tigera

Tigera delivers solutions for secure application connectivity for the cloud native world. Tigera technology is used by the world's largest cloud providers to power connectivity for application development and deployment and to address the connectivity and security challenges that arise in at-scale production. Tigera CNX meets enterprise needs for zero trust network security, multi-cloud and legacy environment support, organizational control and compliance, and operational simplicity. CNX builds on leading open source projects: Kubernetes, Calico, and Istio, which Tigera engineers help maintain and contribute to as active members of the cloud native community.

Tigera, Inc.
58 Maiden Lane, Fl 5
San Francisco
CA 94108

+1 (415) 612-9546
www.tigera.io

All specifications subject to change without notice. Features marked with an asterisk (*) are planned for availability during 1H 2018.

TIGERA